

**IMPLEMENTASI INSTRUCTION DETECTION AND PREVENTION
SYSTEM (IDPS) UNTUK MENDETEKSI SERANGAN PACKET
SNIFFING**

SKRIPSI



disusun oleh

Fadhil Muhammad Ichtibar Suratinoyo

17.11.1537

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021**

**IMPLEMENTASI INSTRUCTION DETECTION AND PREVENTION
SYSTEM (IDPS) UNTUK MENDETEKSI SERANGAN PACKET
SNIFFING**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Sistem Informasi



disusun oleh

Fadhil Muhammad Ichtibar Suratinoyo

17.11.1537

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2021

PERSETUJUAN

SKRIPSI

IMPLEMENTASI INSTRUCTION DETECTION AND PREVENTION SYSTEM (IDPS) UNTUK MENDETEKSI SERANGAN PACKET SNIFFING

yang dipersiapkan dan disusun oleh

Fadhil Muhammad Ichtiyar Suratinoyo

17.11.1537

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 6 Februari 2021

Dosen Pembimbing,

Joko Dwi Santoso
NIK. 190302181

PENGESAHAN

SKRIPSI

IMPLEMENTASI INSTRUTION DETECTION AND PREVENTION SYSTEM (IDPS) UNTUK MENDETEKSI SERANGAN PACKET SNIFFING

yang dipersiapkan dan disusun oleh

Fadhil Muhammad Ichtibar Suratinoyo

17.11.1537

telah dipertahankan di depan Dewan Penguji
pada tanggal 18 Februari 2021

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Joko Dwi Santoso, M.kom
NIK. 190302181

Andriyan Dwi Putra, M.Kom
NIK. 190302270

Nila Feby Puspitaasari, S.Kom, .Cs
NIK. 190302161

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 19 Maret 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.kom
NIK. 190302096

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggung jawab saya pribadi.

Yogyakarta, 18 Maret 2021



Fadhil Muhammad Ichibar Suratimoyo
NIM. 17.11.1537

MOTTO

“Work hard in silence, let success be your noise.”



PERSEMBAHAN

Sujud syukurku kusembahkan kepada ALLAH SWT, Atas takdir mu telah kau jadikan aku manusia yang senantiasa berpikir, Berilmu, Beriman dan bersabar dalam menjalani hidup ini. Semoga keberhasilan ini menjadi satu langkah awal untuk masa depanku, dalam meraih cita-cita yang ingin ku capai.

Dengan ini saya persembahkan karya ini untuk, Umi dan Abi Terima kasih atas kasih sayang yang berlimpah dari mulai saya lahir, hingga saya sudah sebesar ini. Teruntuk Umi dan Abi, terima kasih juga atas limpahan doa yang tak berkesudahan. Serta segala hal yang telah Umi lakukan, semua yang terbaik.

Terima kasih selanjutnya teruntuk kakak, adik, dan keluarga lainya yang selalu membantu dan memotivasi saya agar bisa menyelesaikan skripsi ini dengan cepat. Dan terima kasih juga kepada eman-teman yang tidak bisa saya sebutkan satu persatu, yang selalu menyemangati dan mengingatkan untuk menyelesaikan skripsi, terimakasih telah memberikan semangat dalam hubungan pertemanan yang selama ini terjalin dan waktu yang bisa kita lewati bersama.

KATA PENGANTAR

Puji dan syukur penulis haturkan kepada Allah Subhanahu Wa Ta'ala atas limpahan serta rahmat-Nya lah penulis diberikan kesempatan dan kemudahan dalam menyelesaikan skripsi yang berjudul “ *Implementasi Intrusion Detection And Prevention System (IDPS) Untuk Mendeteksi Serangan Packet Sniffing*”. Sholawat serta salam senantiasa tercurah kepada Rasul junjungan kita Nabi Muhammad Shalallahu 'Alaihi Wasalam.

Penulis juga mengucapkan terima kasih kepada:

1. Bapak M. Suyanto, Prof., Dr., M.M. selaku Rektor Universitas AMIKOM Yogyakarta.
2. Bapak Joko Dwi Santoso, M.Kom. Selaku Dosen pembimbing yang telah memberi arahan dan bimbingan agar penulis dapat menyelesaikan skripsi ini dengan baik.
3. Bapak Joko Dwi Santoso, M.Kom, Bapak Andriyan Dwi Putra, M.kom dan Ibu Nila Feby Puspitasari, S.kom, M.Cs selaku Dosen penguji yang telah menguji penulis sehingga dapat lulus.

Penulis menyadari bahwa laporan akhir masih jauh dari sempurna, oleh karena itu penulis mengharapkan kritik dan saran dari pembaca agar perumusan laporan akhir dapat dilakukan dengan hasil yang lebih baik..

Yogyakarta, 18 Februari 2021

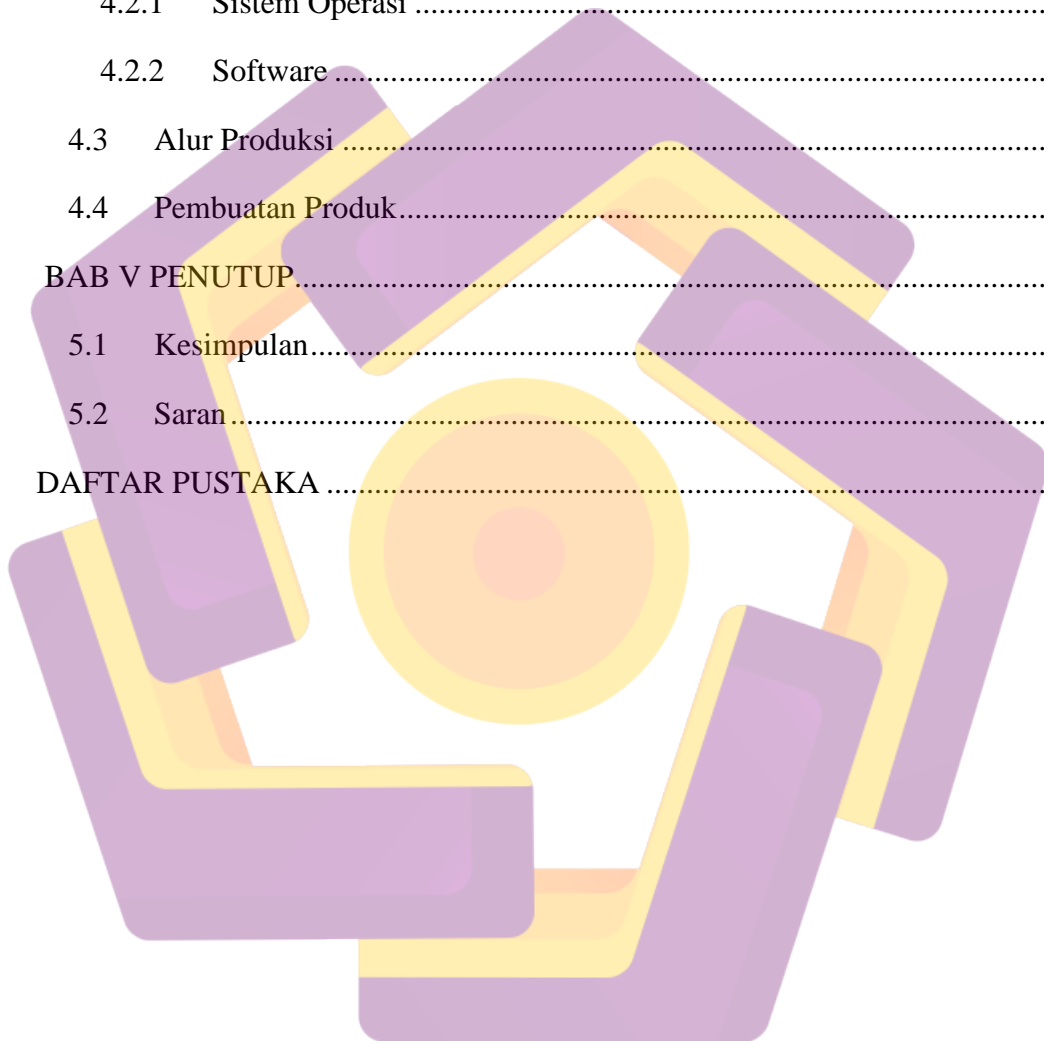
Fadhil Muhammad Ichtibar Suratinoyo

DAFTAR ISI

PERSETUJUAN	i
PENGESAHAN	ii
PENGESAHAN	ii
PERNYATAAN.....	Error! Bookmark not defined.
MOTTO	iv
PERSEMBAHAN.....	v
KATA PENGANTAR	vi
DAFTAR TABLE.....	x
DAFTAR GAMBAR	xi
INTISARI.....	xii
ABSTRACT.....	xiii
BAB I PENDAHULUAN.....	1
1.1 LATAR BELAKANG.....	1
1.2 RUMUSAN MASALAH	1
1.3 BATASAAN MASALAH	1
1.4 TUJUAN PENELITIAN	2
1.5 MANFAAT PENELITIAN.....	2
1.6 METODE PENELITIAN	2
1.6.1 Metode pengumpulan data	2
1.7 SISTEMATIKA PENELITIAN	3
BAB II LANDASAN TEORI	5
2.1 KAJIAN PUSTAKA	5
2.1.1 Penelitian sebelumnya.....	6

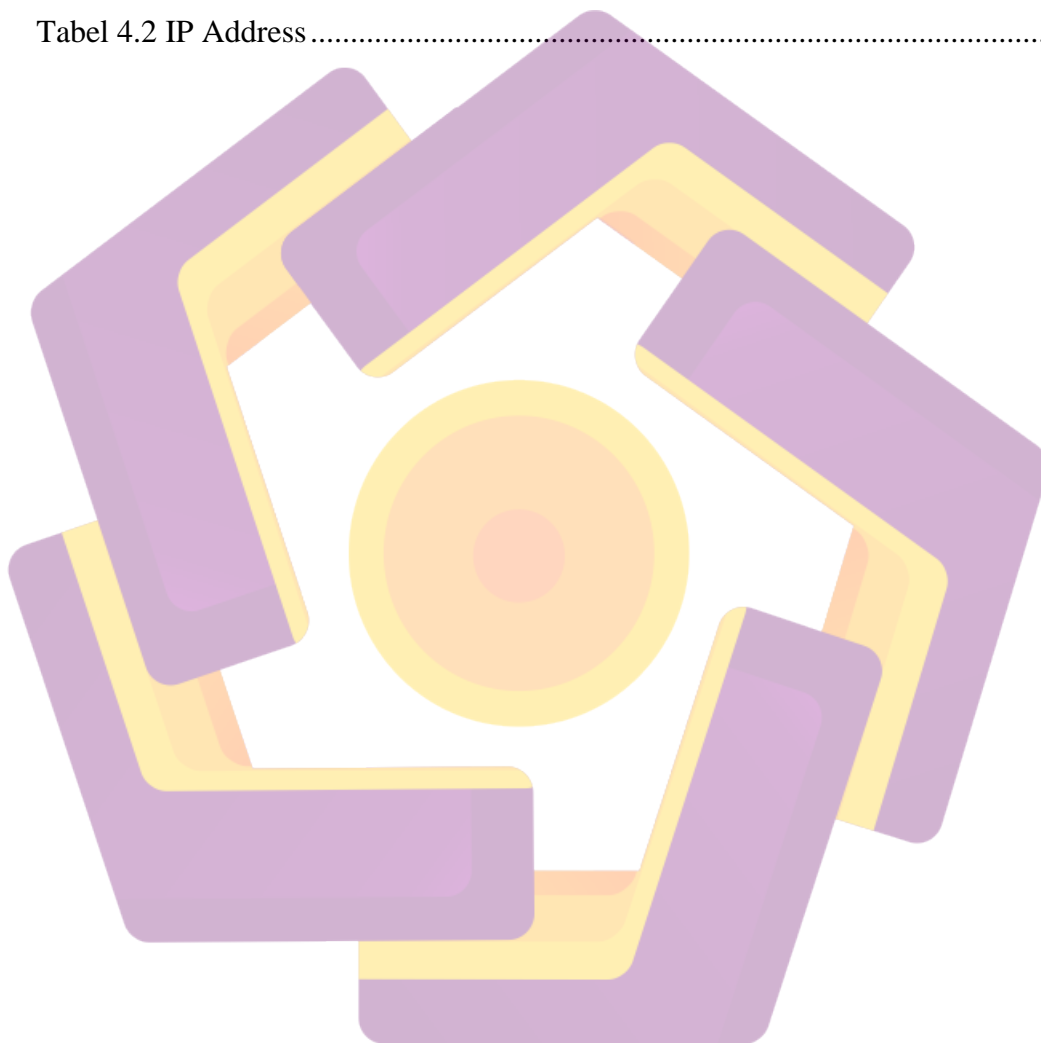
2.2	Dasar Teori	9
2.2.1	Jaringan Komputer	9
2.2.2	Keamanan Jaringan	9
2.2.3	Monitoring jaringan	10
2.2.4	Intrusion Detection And Prevention System (IDPS)	10
2.2.5	Intrusion Detection System (IDS).....	10
2.2.6	Fungsi Intrusion Detection System (IDS)	11
2.2.7	Signature Based IDS	11
2.2.8	Anomaly Based IDS	12
2.2.9	Jenis-jenis Intrusion Detection System (IDS)	12
2.2.10	Intrusion Prevention System (IPS).....	13
2.2.11	Firewall	14
2.2.12	Snort	15
2.2.13	Packet Sniffing	17
2.2.14	ARP	17
2.2.15	ARP Spoofing	18
2.2.16	Security Information and Event Management (SIEM)	19
2.2.17	Splunk	19
2.2.18	Bettercap	20
2.2.19	Nmap (Network Mapper).....	20
2.2.20	Sistem operasi	21
BAB III METODE PENELITIAN.....		22
3.1	Gambaran Umum	22
3.2	Alat dan Bahan Penelitian	23
3.3	Alur Penelitian.....	24

BAB IV HASIL DAN PEMBAHASAN	25
4.1 Rancangan Sistem	25
4.1.1 Perancangan perangkat keras	25
4.2 Perancangan perangkat lunak	25
4.2.1 Sistem Operasi	25
4.2.2 Software	25
4.3 Alur Produksi	26
4.4 Pembuatan Produk.....	26
BAB V PENUTUP.....	54
5.1 Kesimpulan.....	54
5.2 Saran	54
DAFTAR PUSTAKA	55



DAFTAR TABLE

Tabel 2.1 Penelitian Sebelumnya.....	6
Tabel 4.1 perancangan perangkat keras	25
Tabel 4.2 IP Address	25



DAFTAR GAMBAR

Gambar 2.1 Komponen-Komponen Snort (Dar & Harahap, 2018).....	16
Gambar 2.2 Cara kerja Splunk (Abidian & Setiawan, 2021).....	20
Gambar 3.1 Alur Penelitian.....	24
Gambar 4.1 Tampilan Aplikasi VirtualBox	27
Gambar 4.2 Tampilan Sistem Operasi Virtual	27
Gambar 4.3 Tampilan Sistem Operasi Ubuntu Linux Virtual	28
Gambar 4.4 Tampilan Sistem Operasi Kali Linux Virtual	28
Gambar 4.5 Tampilan Versi Snort	32
Gambar 4.6 Hasil Konfigurasi	33
Gambar 4.7 Tampilan IP PC Tampilan IP PC	33
Gambar 4.8 Tampilan Konfigurasi Service	34
Gambar 4.9 Mode Deteksi	35
Gambar 4.10 PuledPork Running	37
Gambar 4.11 Hasil Konfigurasi	38
Gambar 4.12 Alert Format Json	40
Gambar 4.13 Snort Active.....	41
Gambar 4.14 Tampilan Localhost Splunk	43
Gambar 4.15 Snort 3 JSON Alert	43
Gambar 4.16 Skema Jaringan	49
Gambar 4.17 Bettercap Mode Sniffing	50
Gambar 4.18 Hasil Sniffing	51
Gambar 4.19 Hasil Port Scanning.....	51
Gambar 4.20 Alert Pada Splunk.....	52
Gambar 4.21 Hasil Deteksi Serangan	52
Gambar 4.22 Tampilan Port Terlindungi	53
Gambar 4.23 Website Dilindungi oleh Firewall	53

INTISARI

Keamanan jaringan komputer sangat penting untuk diperhatikan, karena jaringan yang terhubung dengan internet pada dasarnya kurang aman dan dapat diserang oleh para penyerang untuk mendapatkan informasi. Karena itu diperlukan sistem keamanan jaringan yang dapat mendeteksi dan mencegah serangan penyusup tersebut.

Penelitian ini menggunakan SDLC. Implementasi sistem Intrusion Detection And Prevention System berbasis snort yang bersifat open source menjadi sebuah keuntungan dari segi biaya dengan performa yang baik dalam mendeteksi serangan. Snort dapat digunakan pada berbagai sistem operasi dan sangat mudah dikonfigurasi sesuai dengan kebutuhan jaringan kita. Serangan dapat terdeteksi atau tidaknya oleh snort, tergantung pada rules pada snort.

Pengujian pendeteksian serangan sniffing dengan menggunakan tools bettercap. Berdasarkan hasil pengujian sistem IDPS berbasis snort dapat mendeteksi dan mencegah adanya upaya penyerangan dan memberikan sebuah alert. Hasil pengujian yang dilakukan diharapkan bisa digunakan sebagai alternatif dalam mengamankan jaringan.

Kata-kunci : IDPS,Packet Sniffing,Snort,Bettercap

ABSTRACT

Computer network security is very important to note, because networks connected to the internet are inherently less secure and can be attacked by attackers for information. Because it requires a network security system that can detect and prevent the intruder's attacks.

This study uses SDLC. The implementation of the Snort-based Intrusion Detection And Prevention System which is open source is a cost advantage with good performance in detecting attacks. Snort can be used on a variety of operating systems and is very easy to configure according to our network needs. The attack can be detected or not by the snort, depending on the rules of the snort.

Testing the detection of sniffing attacks using BetterCap tools. Based on the test results, the snort-based IDPS system can detect and prevent attacks and provide alerts. The results of the tests carried out are expected to be used as an alternative in securing the network.

Keyword: IDPS,,Packet Sniffing,Snort,Bettercap

